REMARKS

Claims 1-26 remain in the application for consideration. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application.

§ 102 Rejections

Claims 1-26 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,052,468 to Hillhouse (hereafter "Hillhouse").

Before undertaking a discussion regarding the substance of the Office's rejections, the following discussion of Hillhouse is included in order to assist the Office in appreciating the patentable distinctions between these references and the claimed subject matter in this application.

The Hillhouse Reference

Hillhouse discloses systems and methods for improving portability of secure encryption key data files by ***re-securing*** key data files according to different security processes for mobility. Specifically, Hillhouse teaches a method of generating secure key databases that is portable to systems having different configurations. Hillhouse also teaches a ***method of selecting a user authentication method from a plurality of user authorization methods for use in securing*** a key data file. Finally, Hillhouse teaches a method of ***securing*** a key database with multiple security methods.

In accordance with Hillhouse's teachings, a key data file comprises a secured cryptographic key which can be secured again according to an authentication method selected from a plurality of available authentication methods available to a user on a particular system. Additionally, the key can be ***re-secured*** over and over again based on selected available authentication methods. The key data is then accessible only via the authentication method(s) used. Thus, the systems and methods in Hillhouse ***control access to key data files by securing a cryptographic key to that file.***

Applicant's Disclosure

Applicant's disclosure provides methods and arrangements for controlling access to resources in a computing environment. These methods and arrangements identify authentication mechanism(s) (and/or characteristics thereof) used in verifying a user to subsequently operating security mechanisms. Thus, additional control is provided by differentiating user requests based on this ***additional information***. For example, in a computer capable of supporting multiple authentication mechanisms, at least one embodiment ***generates an operating system representation*** of at least one ***identity indicator*** associated with at least one authentication mechanism, and subsequently ***controls access*** (to at least one resource) ***based on the operating system representation***. In certain implementations, at least one security identifier that identifies the authentication mechanism in some way can be generated. In other implementations, the operating system representation is compared to at least one access control list (with at least one access control entry). Here, for example, the access control entry may specify ***whether the user authenticated (by the authentication mechanism) is permitted access to the resource.***

Claims Rejected over Hillhouse under § 102

Claim 1 has been amended, and as amended recites a method for use in a computer capable of supporting multiple authentication mechanisms comprising [added language appears in the bold italics]:

- generating at least one indicator ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism that has been used to authenticate ***the*** user; and
- controlling ***the user's*** access to at least one resource based on the indicator.

In making the rejection, the Office argues that Hillhouse discloses generating at least one indicator associated with and identifying at least one authentication mechanism that has been used to authenticate a user (citing column 8 lines 1-15, column 8, lines 27-43, and column 8 line 65 to column 9 line 6) and controlling access to at least one resource based on the indicator (citing column 5 lines 32-38, and column 8 lines 35-43).

In order to clarify the recited subject matter, this claim has been amended to clarify generating at least one indicator ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism ***that has been used to authenticate the user, and controlling the user's access to at least one resource based on the indicator.*** Support for this amendment can be found in the Applicant's specification on page 7. Of course, this example from the specification is but one example of the subject matter that is embodied by this claim and in no way limits claim 1. In light of the current amendments, Applicant respectfully traverses the Office's rejections.

The excerpt cited by the Office at column 8, lines 27-43, merely discusses a method in which code two bytes in length ***indicates the type of authentication method*** (i.e., fingerprint, password, etc.) that must be used in order to gain access to a key file comprising a cryptographic key. The indicator does not indicate that the user has been authenticated. The excerpt from column 8 is reproduced below:

> According to one embodiment the data indicative of a user authorization method comprises a sequence of bytes including a length for indicating, one of the data length and the number of authentication methods employed to secure the key data ***and an indicator of a user authentication method comprising a number, for example 2 bytes, unique to each available method.*** Typically two bytes are used to identify the method selected thereby allowing for over 65,000 different user authentication methods. ***This permits the implementation of variations on user authentication methods to increase the difficulty of breaking the security of the key data.***

Furthermore, the excerpt cited by the Office at column 8 lines 1-15 merely teaches that one user may be authenticated and then subsequently access a key and then select an authentication method that must be used by a second user in order to access the same key. The second user may only access the key after being authenticated by the method chosen by the first user. This excerpt is reproduced below for the convenience of the Office:

> In accordance with the invention, a method is provided to provide secure access to encrypted data by each of a plurality of people. Accordingly, ***a user determines to secure a key data file*** comprising a secured cryptographic key. ***The user is authenticated*** and the cryptographic key is accessed. ***The user selects an authentication method*** in the form of a biometric authentication method such as a fingerprint, a voiceprint, a face, a palm print, a retinal scan, and so forth; a password; or a key. The authentication method is selected from a plurality of available authentication methods. ***Another user is authenticated according to the selected method and the secured cryptographic key is secured according to that method.*** The secured cryptographic key is stored in a second other key data file with data relating to the selected authorization method.

> Alternatively, the key data is stored in a same file along with the previous secure key data. This allows for user authentication of any of a plurality of individuals providing access to same key data.

Thus, while there appears to be some type of indicator that indicates the type of authentication method that must be used by the second user to access the key, there is no mention whatsoever in this excerpt of an indicator that ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism ***that has been used to authenticate the user, <u>and</u> controlling <u>the user's</u> access to at least one resource based on the indicator.***

Furthermore, the excerpt cited by the Office at column 8 line 65 – column 9 line 6 merely states that there are many types of authorization methods that each have a unique identifier. This excerpt is reproduced below for the convenience of the Office:

> Of course, ***many different fingerprint analysis methods may be employed, each having a unique authorization method identifier.*** Therefore, provision of a fingerprint is not indicative of the biometric authorization method ***whereas the authorization method is indicative of necessary user input.*** Similarly, many methods of extracting a key from a password are known and, according to the present invention, those implemented each have a unique authorization method identifier.

Again, this excerpt does not mention an indicator ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism ***that has been used to authenticate the user.***

In light of the current amendments, the excerpts cited by the Office neither disclose nor suggest the subject matter of this claim. Accordingly, for at least this reason, this claim is allowable.

Claims 2-10 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested by the reference of record.

Claim 11 has been amended, and as amended recites a computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising [added language appears in the bold italics]:

- producing at least one indicator that ***identifies a user, and*** uniquely identifies at least one authentication mechanism supported by the device ***that has been used to authenticate the user***; and
- causing the device to selectively control ***the user's*** access to at least one resource operatively coupled to the device based at least in part on the indicator.

In making the rejection of claim 11, the Office uses much the same argument as used in making out a rejection of claim 1. The Applicant has made similar amendments in claim 11 as made in claim 1. In light of the current amendments, and for the same reasons as discussed by the Applicant with regards to claim 1, the Applicant respectfully traverses the Office's rejections. Accordingly, this claim is allowable.

Claims 12-20 depend from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither shown nor suggested by the reference of record.

Claim 21 has been amended, and as amended recites an apparatus comprising [added language appears in the bold italics]:

- at least one authentication mechanism configured to generate at least one indicator that ***identifies a user, and*** identifies the authentication mechanism ***that has been used to authenticate the user***;
- an access control list;
- at least one access controlled resource; and
- logic operatively configured to compare the indicator with the access control list and selectively control ***the user's*** access to the resource based on the indicator.

In making the rejection of claim 21, the Office uses much the same argument as used in making out a rejection of claim 1. The Applicant has made similar amendments in claim 21 as made in claim 1. In light of the current amendments, and for the same reasons as discussed by the Applicant with regards to claim 1, the Applicant respectfully traverses the Office's rejections. Accordingly, this claim is allowable.

Claims 22-26 depend from claim 21 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 21, are neither shown nor suggested by the reference of record.

<u>Conclusion</u>

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 2/15/06

By:

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256